REMARKS

The Examiner has rejected Claims 5-7 and 29-31 under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. Applicant respectfully disagrees with such rejection, but has cancelled such claims in order to expedite the prosecution of the present application.

The Examiner has rejected Claims 1-2, 4-7, 10, 14-26, 28-31, 34, 38-53 and 55 under 35 U.S.C. 112, second paragraph, as being indefinite. Applicant respectfully asserts that such rejections are avoided in view of the clarifications made to each of the independent claims.

The Examiner has rejected Claims 1-2, 4-7, 10, 14-18, 20, 24-26, 28-31, 34, 38-42, 44, 50 and 53 under 35 U.S.C. 103(a) as being unpatentable over Muttik (U.S. Patent No. 6,775,780), in view of Bowlin (U.S. Patent Application Publication No. 2002/0099944), and in further view of Hutchison (U.S. Patent No. 6,457,022). The Examiner has also rejected Claims 19, 21-23, 42, 45-47, 51 and 52 under 35 U.S.C. 103(a) as being unpatentable over Muttik, in view of Bowlin, in further view of Hutchison, and in further view of Schnurer (U.S. Patent No. 5,842,002). The Examiner has still further rejected Claim 55 under 35 U.S.C. 103(a) as being unpatentable over Muttik, in view of Bowlin, in further view of Hutchison, in further view of Schnurer, in further view of Porras (U.S. Patent No. 6,704,874), in further view of Conklin (U.S. Patent No. 5,991,881), and in further view of Boate (U.S. Patent Application Publication No. 2002/0104006).

Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to substantially incorporate the subject matter of Claim 55.

With respect to independent Claims 1, 24 and 50-52, the Examiner has relied on paragraph [0038] and Figure 6 in Bowlin along with Col. 3, lines 30-42 and Figure 1 in Muttik, as excerpted below, to make a prior art showing of applicant's claimed "running a computer on a network in an opened share mode, wherein the opened share mode indicates a file structure parameter and a name parameter and applies only to a manually selected list of at least one of application programs and data" (Claims 1, 24 and 50), and "the actual opened share mode indicates a file structure parameter and a name parameter that are capable of actually being accessed by the other computers, and applies only to a manually selected list of at least one of application programs and data" (Claims 51 and 52).

> "To make the selections for the safe zone, the user may be presented with a display screen 600 such as the one illustrated in FIG. 6. The display screen 600 may, for example, mimic an operating system's own method of displaying files and directories to a user (e.g., Microsoft.RTM.'s Windows Explorer). **The user may be able to select files and/or entire directories for the safe zone** by simply marking the check boxes (e.g., 610, 620 and 630) which are associated with files and directories presented on the computer display screen 104. The check boxes may be marked using an appropriate input device 310 associated with the computer system 100 (e.g., mouse 108, keyboard 106, pen tablet, touch screen, or trackball). For example, FIG. 6 shows that the user has selected for the safe zone two individual files (FILE1 and FILE2) and an entire directory (PROJECTS) by marking the check boxes 610, 620 and 630. Alternatively, other methods of selecting the files and/or directories to be included in the safe zone are possible. For example, the selections could be made by the user uttering voiced responses." (Bowlin [0038]-emphasis added)

> "**Computer system 106 receives code 108 (which can potentially be malicious) from a number of different sources.** Code 108 may be introduced into computer system 106 by a remote host 101 across a network 102. For example, code 108 may be included in an electronic mail (email) message from remote host 101 to computer system 106. Remote host 101 can be any entity that is capable of sending code 108 across network 102. Network 102 can include any type of wire or wireless communication channel capable of coupling together computing nodes. This includes, but is not limited to, a local area network, a wide area network, or a combination of networks. In one embodiment of the present invention, network 102 includes the Internet." (Muttik Col. 3, lines 30-42-emphasis added)

The Examiner has further stated in his response to applicant's arguments filed 6/2/05 that "[t]he system runs in a shared mode in which files not checked are allowed to

be accessed by network applications and a virtual shared mode in which files checked are safeguarded from access by network applications." However, applicant claims that the "opened share mode...applies only to a manually selected list of at least one of application programs and data" (emphasis added). Thus, the Examiner has essentially admitted that Bowlin discloses a shared mode in which files not checked (i.e. not selected) are allowed to be accessed and that the virtual shared mode requires files to be checked, which is the exact opposite of applicant's specific claim language. Thus, Bowlin clearly *teaches away* from applicant's claimed invention.

To emphasize, applicant respectfully asserts that such excerpt in Bowlin only teaches "selecting files and/or entire directories for the safe zone" (see emphasized excerpt above). However, such safe zone limits access to files and/or directories in the safe zone according to selected authorized accesses, whereas files and/or directories not in the safe zone are automatically granted access. See paragraph [0026] in Bowlin. Thus, Bowlin's safe zone does not meet applicant's claimed opened share mode.

With respect to independent Claims 1, 24 and 50-52, the Examiner has relied on Col. 2, lines 9-11 in Muttik, as excerpted below, to make a prior art showing of applicant's claimed "determining whether the applications attempt to modify the computer (see this or similar, but not identical language in each of the foregoing claims).

> "Based upon this comparison, the system determines whether the software is likely to exhibit malicious behavior." (Col. 2, lines 9-11).

Applicant respectfully asserts that simply determining software "to be likely to exhibit malicious behavior," as in the excerpt above (emphasis added), does not meet applicant's specific claim language. In particular, applicant claims "determining whether the applications attempt to modify the computer" (emphasis added), and not merely whether they are likely to exhibit malicious behavior, as in Bowlin.

With respect to independent Claims 1, 24 and 50, the Examiner has relied on paragraph [0038] in Bowlin along with Col. 8, lines 22-25 in Hutchison, as excerpted in

part above, to make a prior art showing of applicant's claimed technique "wherein the opened share mode indicates a plurality of parameters that are randomly selected to prevent detection." Again, applicant respectfully asserts that only the safe mode in Bowlin, which limits access to files, indicates authorized accesses, and simply does not meet the opened share mode, as claimed by applicant.

With respect to independent Claims 51 and 52, the Examiner has relied on paragraph [0038] and Figure 6 in Bowlin along with Col. 3, lines 30-42 and Figure 1 in Muttik, as excerpted above, to make a prior art showing of applicant's claimed "running a computer on a network in a virtual opened share mode and an actual opened share mode, wherein the virtual opened share mode allows other computers on the network to access predetermined data and programs resident on the computer, and indicates to other computers of an ability to write to the computer" (see this or similar, but not identical language in each of the foregoing claims).

Applicant respectfully asserts that the excerpt from Bowlin relied on by the Examiner merely teaches "select[ing] files and/or entire directories for the safe zone." Simply selecting files and/or directories for a safe zone does not even suggest a "virtual opened share mode [that]...indicates to other computers of an ability to write to the computer," as claimed by applicant. In fact, applicant asserts that the only permissions indicated with respect to the safe zone in Bowlin relate to types of "authorized accesses (e.g. application accesses, process accesses, service accesses, system agent and user accesses, etc.)" (see paragraph [0026]), and not to "an ability to write to the computer," as specifically claimed by applicant.

Still with respect to independent Claims 51 and 52, the Examiner has relied on Col. 1, lines 66-67; Col. 2, lines 1-11; and Figure 1 in Muttik along with paragraph [0026] in Bowlin to make a prior art showing of applicant's claimed "monitoring attempts to access the computer by applications utilizing the network, using, at least in part, the file structure and name parameter" (see this or similar, but not identical language in each of the foregoing claims).

Applicant respectfully asserts that the excerpts in Muttik relied on by the Examiner merely teach "determining whether software is likely to exhibit malicious behavior" (emphasis added). In addition, the excerpt in Bowlin relied on by the Examiner simply teaches determining whether grant access to a file. Clearly, neither reference discloses "monitoring attempts to access the computer by applications utilizing the network," as specifically claimed by applicant (emphasis added).

Also with respect to independent Claims 51 and 52, the Examiner has relied on Col. 1, line 66-Col. 2 line 11 from Muttik to make a prior art showing of applicant's claimed technique "wherein any attempt to modify the computer is utilized in a heuristic analysis for identifying a coordinated attack on multiple computers" (see this or similar, but not identical language in each of the foregoing claims). Applicant respectfully asserts that such excerpt merely generally teaches "determining whether software is likely to exhibit malicious behavior" (emphasis added), and not "any attempt to modify the computer ... utilized... for identifying a coordinated attack on multiple computers" (emphasis added).

Further, with respect to independent Claims 51 and 52, the Examiner has relied on paragraph [0026] in Bowlin and Col. 8, lines 26-35 in Schnurer to make a prior art showing of applicant's claimed technique "wherein (d)-(h) are carried out if it is determined that the applications attempt to modify the computer via the virtual opened share mode; and access is permitted if it is determined that the applications attempt to modify the computer via the actual opened share mode."

Applicant respectfully asserts that Bowlin only discloses that if "the request [to access a file] is determined to be unauthorized, access to the file is denied." However, nowhere in Bowlin is there any teaching of acting in the manner claimed by applicant "if it is determined that the applications attempt to modify the computer via the virtual opened share mode." Also, the excerpt in Schnurer relied on by the Examiner only

relates to the detection of a virus, and not "applications [that] attempt to modify the computer via the virtual opened share mode."

In addition, with respect to independent Claims 51 and 52, the Examiner has relied on paragraph [0038] in Bowlin and Col. 8, lines 22-24 in Hutchison to make a prior art showing of applicant's claimed "wherein the parameters are randomly selected to prevent detection." Applicant respectfully asserts that Bowlin simply teaches selecting files and/or directories for a safe zone and Hutchison simply teaches permissions for files. Clearly, neither excerpt discloses any sort of "parameters [that] are randomly selected to prevent detection," as claimed by applicant (emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claim 55 into each of the independent claims, as well as emphasize that the parameters of applicant's claimed invention are randomly selected "to prevent detection of a virtuality of the parameters," as now claimed by applicant.

With respect to Claim 55, the subject matter of which is presently incorporated into each of the independent claims, the Examiner has relied on paragraph [0042] in Boate to make a prior art showing of applicant's claimed "logging the computer back on the network in a mode other than the actual opened share mode" (see this or similar but not identical language in each of the independent claims). Applicant respectfully asserts that Boate simply teaches resuming operation of an application if a user's PDI is detected within a short second predetermined time period. However, such PDI is not logged "back on the network," as claimed by applicant, let alone "in a mode other than the actual opened share mode."

Also with respect to Claim 55, the Examiner has relied on Col. 8, lines 26-35 in Schnurer to make a prior art showing of applicant's claimed "sending an alert and logging a culpable computer off the network based on the determination" (see this or similar but not identical language in each of the independent claims). However, applicant notes that the actions described in the Schnurer excerpt relied on by the Examiner only relate to a detection of a virus, and NOT to the specific determination claimed by applicant, namely "a trend [that] is found indicative of a coordinated attack" (emphasis added).

Since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a specific prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are

enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P019/01.096.01).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100